David C. O'Mara Nevada Bar No. 8599 THE O'MARA LAW FIRM, P.C. 311 E. Liberty Street Reno, Nevada 89501 775.323.1321 www.omaralaw.net

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: (312) 621-2000

*pro hac vice forthcoming

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT DISTRICT OF NEVADA

THOMAS MCNICHOLAS and LAURA MCNICHOLAS, individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

CAESARS ENTERTAINMENT, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Thomas McNicholas and Laura McNicholas (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this Class Action Complaint against Caesars Entertainment, Inc. ("Caesars") and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

- 1. Plaintiffs bring this class action against Caesars for its failure to secure and safeguard their and other individuals' personally identifiable information ("PII"), including driver's license numbers and Social Security numbers.
- 2. Caesars is a large gaming company headquartered in Reno, Nevada. The company claims to be "the largest gaming company in the U.S." and "the global leader in the gaming industry."
- 3. On September 7, 2023, Caesars reported to the United States Securities and Exchange Commission ("SEC") that unauthorized individuals had access to its network systems and acquired the PII of Plaintiffs and Class members (the "Data Breach").
- 4. Caesars owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Caesars breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect Plaintiffs' and Class members' PII from unauthorized access and disclosure.
- 5. As a result of Caesars's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII was exposed as a result of the Data Breach.
- 6. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, negligence per se, breach of implied contract, unjust enrichment, and violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, and seek declaratory relief,

¹ See Caesars Entertainment, https://www.caesars.com/corporate (last accessed Sep. 21, 2023).

injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiffs Thomas and Laura McNicholas

- 7. Plaintiffs Thomas and Laura McNicholas are citizens of the State of Illinois.
- 8. Plaintiffs were required to provide their PII to Caesars in connection with joining the Caesars Rewards Program. Plaintiffs have been members of the Caesars Rewards Program for over twenty years.
- 9. Based on representations made by Caesars, Plaintiffs believed that Caesars had implemented and maintained reasonable security and practices to protect their PII. With this belief in mind, Plaintiffs provided their PII to Caesars in connection with or in exchange for services related to the Caesars Rewards Program.
- 10. In connection with services provided to Plaintiffs, Caesars stores and maintains Plaintiffs' PII on their systems, including the systems involved in the Data Breach.
- 11. Had Plaintiffs known that Caesars does not adequately protect the PII in its possession, they would not have agreed to provide Caesars with their PII.
- 12. As a direct result of the Data Breach, Plaintiffs have suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of their highly sensitive PII; deprivation of the value of their PII; and overpayment for services that did not include adequate data security.

Defendant Caesars Entertainment, Inc.

13. Defendant Caesars Entertainment, Inc. is a corporation formed under the laws of Delaware. Caesars's principal place of business is located at 100 West Liberty Street, 12th Floor,

Reno, Nevada 89501. Caesars can be served via its registered agent, Corporation Service Company, 112 North Curry Street, Carson City, Nevada 89703.

JURISDICTION AND VENUE

- 14. The Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds \$5,000,000, exclusive of interest and costs.
- 15. This Court has personal jurisdiction over Caesars because Caesars has its principal place of business in Nevada and does significant business in Nevada.
- 16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Caesars has its principal place of business in Washoe County, Nevada, and a substantial part of the events giving rise to Plaintiffs' claims arose in this District.

FACTUAL ALLEGATIONS

Overview of Caesars

- 17. Caesars is one of the largest gaming companies in the world, reporting over \$33 Billion in assets to the SEC in its June 30, 2023 report.² The company has over 50 resorts worldwide.³
- 18. In the regular course of its business, Caesars collects and maintains the PII of its customers.
 - 19. Caesars maintains a privacy policy directed to its customers (the "Privacy Policy")

² Form 10-Q, U.S. SEC. AND EXCH. COMM'N (Aug. 1, 2023), https://www.sec.gov/ix?doc=/Archives/edgar/data/1590895/000159089523000091/czr-20230630.htm (last accessed Sep. 21, 2023).

³ See Caesars Entertainment, supra, n.1.

which states: "Caesars Entertainment, Inc. and its subsidiaries and affiliates . . . are committed to respecting your data privacy." The Privacy Policy also states, "We maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control."

20. Plaintiffs and Class members are, or were, customers or Rewards Members of Caesars and entrusted Caesars with their PII.

The Data Breach

- 21. Prior to September 7, 2023, unauthorized individuals gained access to Caesars's network systems. The Data Breach was a ransomware attack, and it has been reported that Caesars paid the cybercriminals approximately \$15 million. Caesars reports that the unauthorized individuals acquired a copy of, "among other data, [its] loyalty program database," which included the PII of Plaintiffs and Class members. Caesars's report states that it has "taken steps to ensure that the stolen data is deleted by the unauthorized actor, although we cannot guarantee the result." The Data Breach has left Plaintiffs and Class members at an imminent risk of fraud and identity theft, if they have not already experienced them.
 - 22. Despite the fact that the Data Breach occurred at some time prior to September 7,

⁴ Caesars Entertainment, Inc. U.S. Privacy Policy, CAESARS, https://www.caesars.com/corporate/privacy (last accessed Sep. 21, 2023).

⁵ *Id*.

⁶ See Form 8-K, U.S. SEC. AND EXCH. COMM'N (Sep. 7, 2023), https://www.sec.gov/Archives/edgar/data/1590895/000119312523235015/d537840d8k.htm.

⁷ Sergiu Gatlan, Caesars Entertainment Confirms Ransom Payment, Customer Data Theft, BLEEPINGCOMPUTER (Sep. 14, 2023 12:58 PM), https://www.bleepingcomputer.com/news/security/caesars-entertainment-confirms-ransom-

payment-customer-data-theft/.

⁸ See Form 8-K, supra, n.6.

⁹ *Id*.

2023, Plaintiffs believe that Caesars has yet to send notification of the Data Breach to its customers. Thus, Plaintiffs' and Class members' PII has already been in the hands of cybercriminals for weeks without any direct notification to Plaintiffs and Class members.

23. Caesars's SEC filing states the information that was disclosed included "driver's license numbers and/or social security numbers for a significant number of members in the database" and that it is "still investigating the extent of any additional personal or otherwise sensitive information contained in the files acquired by the unauthorized actor." ¹⁰

Caesars Knew that Criminals Target PII

- 24. At all relevant times, Caesars knew, or should have known, that the PII that it collected was a target for malicious actors. Despite such knowledge, Caesars failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII from cyber-attacks that Caesars should have anticipated and guarded against.
- 25. It is well known among companies that store sensitive personally identifying information that such information—such as the Social Security numbers ("SSNs") and financial information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers Many of them were caused by flaws in ... systems either online or in stores."¹¹

¹⁰ *Id*.

¹¹ Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

- 26. PII is a valuable property right.¹² "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."¹³ American companies are estimated to have spent over \$19 billion on acquiring personal data of consumers in 2018.¹⁴ PII is so valuable to identity thieves that once it has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.
- 27. Identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches including the information exposed in the Data Breach can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.
- 28. Consumers place a high value on the privacy of their data, as they should. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites." ¹⁵

¹² See Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED. FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible..."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

¹³ OECD, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data 5k486qtxldmq-en.

¹⁴ IAB Data Center of Excellence, *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

¹⁵ Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

29. Given these facts, any company that transacts business with a consumer and then compromises the privacy of the consumer's PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

- 30. Theft of PII can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.¹⁶ 17
- 31. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.¹⁸

¹⁶ See Federal Trade Commission, What to Know About Identity Theft, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Sep. 21, 2023).

¹⁷ The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

¹⁸ See Louis DeNicola, What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

- 32. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.¹⁹
- 33. Theft of SSNs also creates a particularly alarming situation for victims because SSNs cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of her SSN. Thus, a new SSN will not be provided until after the harm has already been suffered by the victim.
- 34. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. *TIME* quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."²⁰
- 35. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a victim discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some victims up to three years to learn that information.²¹
- 36. Paying a ransom in the case of a ransomware attack does little to mitigate the damage of a data breach. The FBI has stated that it "does not support paying a ransom in response

¹⁹ Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Sep. 21, 2023).

²⁰ Patrick Lucas Austin, 'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

²¹ John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

to a ransomware attack."²² It cautions companies that "paying a ransom doesn't guarantee you or your organization will get any data back."²³

37. It is within this context that Plaintiffs and Class members must now live with the knowledge that their PII is forever in cyberspace, having been stolen by criminals willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Damages Sustained by Plaintiffs and the Other Class members

38. Plaintiffs and Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased and imminent risk of identity theft—risk which justifies or necessitates expenditures for protective and remedial services, for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

CLASS ACTION ALLEGATIONS

- 39. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.
- 40. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

²² Ransomware, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed Sep. 21, 2023).

 $^{^{23}}$ Id.

All persons whose personally identifiable information was accessed in the Data Breach by unauthorized persons, including all who are sent a notice of the Data Breach.

- 41. Excluded from the Class is Caesars Entertainment, Inc., and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).
- 42. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.
- 43. The members of the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Caesars's SEC filing on the Data Breach stated that the unauthorized individuals copied the loyalty program database.²⁴ While Caesars has not yet confirmed the number of persons affected by the Data Breach, the company stated in an April 22, 2022 press release that the company had 65 million members in its loyalty program.²⁵
- 44. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:
 - a. whether Caesars had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members'
 PII from unauthorized access and disclosure;

²⁴ See Form 8-K, supra, n.6.

²⁵ Caesars Entertainment's Loyalty Program, Caesars Rewards, Wins for "Best Customer Service" and "Best Promotion" at Prestigious Freddie Awards on April 21, CAESARS (Apr. 22, 2022), https://investor.caesars.com/news-releases/news-release-details/caesars-entertainments-loyalty-program-caesars-rewardsr-wins.

- b. whether Caesars failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII;
- c. whether an implied contract existed between Class members and Caesars, providing that Caesars would implement and maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;
- d. whether Caesars breached its duties to protect Plaintiffs' and Class members'
 PII; and
- e. whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.
- 45. Caesars engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.
- 46. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Caesars, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.
- 47. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with

substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

48. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Caesars, so it would be impracticable for Class members to individually seek redress from Caesars's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I NEGLIGENCE

- 49. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.
- 50. Caesars owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting the PII in Caesars's possession, custody, or control.
- 51. Caesars knew or should have known the risks of collecting and storing Plaintiffs' and Class members' PII and the importance of maintaining secure systems. Caesars knew or should have known that it faced an increased threat of customer data theft, as judged by the many data breaches that targeted companies that stored PII in recent years.

- 52. Given the nature of Caesars's business, the sensitivity and value of the PII they maintain, and the resources at their disposal, Caesars should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.
- 53. Caesars breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs and Class members' PII by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiffs' and Class members' PII.
- 54. It was or should have been reasonably foreseeable to Caesars that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.
- 55. But for Caesars's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been compromised.
- 56. As a result of Caesars's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft—risk justifying or necessitating expenditures for protective and remedial services for which they are

entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

<u>COUNT II</u> NEGLIGENCE PER SE

- 57. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.
- 58. Caesars's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair... practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Caesars, of failing to employ reasonable measures to protect and secure PII.
 - 59. Caesars's violation of Section 5 of the FTCA constitutes negligence per se.
- 60. Plaintiffs and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.
- 61. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and Class members as a result of the Data Brach.
- 62. It was reasonably foreseeable to Caesars that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor,

and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.

63. The injury and harm that Plaintiffs and Class members suffered was the direct and proximate result of Caesars's violations of Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft—risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III BREACH OF IMPLIED CONTRACT

- 64. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.
- 65. In connection with the dealings Plaintiffs and Class members had with Caesars, Plaintiffs and Class members entered into implied contracts with Caesars.
- 66. Pursuant to these implied contracts, Plaintiffs and Class members provided Caesars with their PII, directly or indirectly, in order for Caesars to provide services or products. In exchange, Caesars agreed to, among other things, and Plaintiffs and Class members understood that Caesars would: (1) provide services or products to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of

Plaintiffs' and Class members' PII; and (3) protect Plaintiffs' and Class members' PII in compliance with federal and state laws, regulations, and industry standards.

- 67. The protection of PII was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Caesars, on the other hand. Indeed, Caesars was clear in its representations in its Privacy Policy, and on that basis of those representations Plaintiffs understood that, Caesars supposedly respects and is committed to protecting customer privacy.
- 68. Had Plaintiffs and Class members known that Caesars would not adequately protect its customers' and former customers' PII, they would not have provided Caesars with their PII.
- 69. Plaintiffs and Class members performed their obligations under the implied contracts when they provided Caesars with their PII, either directly or indirectly.
- 70. Caesars breached its obligations under its implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.
- 71. Caesars's breach of its obligations of the implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.
- 72. Plaintiffs and all other Class members were damaged by Caesars's breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased and imminent risk of identity theft—

a risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

COUNT IV UNJUST ENRICHMENT

- 73. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.
 - 74. This claim is pleaded in the alternative to the breach of implied contract claim.
- 75. Plaintiffs and Class members conferred a monetary benefit upon Caesars in the form of monies paid for services or products to Caesars.
- 76. Caesars accepted or had knowledge of the benefits conferred upon them by Plaintiffs and Class members. Caesars also benefitted from the receipt of Plaintiffs' and Class members' PII, as this was used in providing products and services.
- 77. As a result of Caesars's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.
- 78. Caesars should not be permitted to retain the money belonging to Plaintiffs and Class members because Caesars failed to adequately implement the data privacy and security

procedures that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

79. Caesars should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/2, et seq. ("ICFA")

- 80. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.
- 81. Caesars offered and continues to offer products and services in the State of Illinois.
- 82. Plaintiffs and Class members purchased and received services from Caesars for personal, family, or household purposes.
- 83. Caesars engaged in unlawful and unfair practices in violation of the ICFA by failing to implement and maintain reasonable security measures to protect and secure its customers' PII in a manner that complied with applicable laws, regulations, and industry standards.
- 84. Caesars makes explicit statements to its customers in its Privacy Policy that their PII will remain private.
- 85. Caesars's duties also arise from the Illinois Personal Information Protection Act, 815 ILCS 530/45(a) which states:

A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect

those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS 530/45. Caesars violated this duty by failing to implement reasonably secure data security policies.

- 86. Caesars further violated the ICFA by failing to notify Plaintiffs and Class members of the data breach in a timely manner. The Illinois Personal Information Protection Act requires entities that experience a data breach to notify Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10. Violation of the Illinois Personal Information Protection Act constitutes an unlawful practice under the ICFA. 815 ILCS 530/20.
- 87. Due to the Data Breach, Plaintiffs and Class members have lost property in the form of their PII. Further, Caesars's failure to adopt reasonable practices in protecting and safeguarding its customers' PII will force Plaintiffs and Class members to spend time or money to protect against identity theft. Plaintiffs and Class members now face a high risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Caesars's practice of collecting and storing, or contracting with companies that collect and store, PII without appropriate and reasonable safeguards to protect such information.
- 88. As a result of Caesars's violations of the ICFA, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Caesars's possession; (vi) future costs in terms of time, effort, and money that will be required to

prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

PRAYER FOR RELIEF

Plaintiffs, individually, and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Caesars as follows:

- A. certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;
- B. awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;
- C. awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Caesars from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;
- D. awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;
- E. awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and
- F. awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: September 22, 2023 Respectfully submitted,

/s/ DAVID C. O'MARA, ESQ.

David C. O'Mara Nevada Bar No. 8599 THE O'MARA LAW FIRM, P.C. 311 E. Liberty Street Reno, Nevada 89501 775.323.1321 david@omaralaw.net

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: (312) 621-2000
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiffs and the Proposed Class

^{*}pro hac vice forthcoming